Privacy Practices for Competitive Advantage Part 2

April 07, 2008

Mary Beth Joublanc

www.azgita.gov/sispo

Privacy is the goal
Security is the journey
Technology can help
People are the key

Agenda

- Privacy IS Good Business!
- Arizona on the “Privacy” Grid
- What Should be in Your Privacy Plan

Mary Beth Joublanc – BIO Highlights

- Arizona's Chief Privacy Officer
  - Appointed January 15, 2007
  - Licensed AZ Attorney & member of AZ State Bar
- Chief Health Insurance Portability and Accountability Act (HIPAA) Compliance Officer (ADHS)
  - Created HIPAA Privacy and Security compliance program
  - Member of the Statewide HIPAAZ Workgroup
  - Chairperson Human Subjects Research Review Board
- Appointee to National Academy of Science, Institute of Medicine Committee on HIPAA and Research

Privacy IS Good Business!

- Trust = Goodwill=$$
- Privacy culture empowers employees and reduces turnover
  - Respect
  - Participation
- Privacy Plan is integrated with business strategies and operations

Arizona on the Privacy Grid

- Individual Rights through Regulation (same as federal government)
- AZ Health Information laws and the federal Health Insurance Portability and Accountability Act (HIPAA)
  (ARS 12-2291-12-2297; 45 CFR 160, 162, 164)
- Social Security Number Protection
  (ARS 44-1373 – 1373.03)
- Breach Notification Law (ARS 44-7501)

A.R.S. 44-7501

- Notification of Breach of Security System:
  - Conducts business in AZ
  - Owns, licenses, maintains unencrypted computer data
  - If "becomes aware" of unauthorized acquisition and access involving unencrypted or unredacted "personal information"
  - Promptly investigate
  - Expedient notification (exception for criminal investigation
  - Excludes: Gramm, Leach, Bliley Act and HIPAA

A.R.S. 44-7501

- Personal Information:
  - First name or initial and last name
  - SSN
  - Driver's License number
  - Non-operating ID
  - Financial account number, credit card number, debit card number with security, access code or password

A.R.S. 44-7501

- Redact:
  - Alter or truncate
  - No more than last 4 digits of SSN, driver's license or non-operating license number, financial account number or credit/debit card number
  - Combined with other personal information

A.R.S. 44-1373 through 44-1373.03

- Restricted Use of Personal Identifying Information—Social Security Number
  - May not disclose to general public
  - Cannot be on a card for products or services
  - Can't Require transmission over Internet unless a secure connection or SSN is encrypted
  - Can't require for access to Internet web site unless password, PIN or other unique identifier is also required.

A.R.S. 44-1373 through 44-1373.03

- Prohibitions on printed materials
- Exception if required by law or for internal verification or administrative purposes
- Government agencies not to use as an ID (Exceptions for law enforcement, Department of Revenue with certain limitations)
- Limitations on transmissions to individuals
- Can use last 4 or 5 numbers of SSN

E-Discovery

- Federal rules of procedure have adopted (coming to AZ)
  - duty to preserve and produce electronically stored information for pending or actual litigation
  - Emails must be preserved
  - Plan to classify and retain

Your Privacy Plan

- Executive Management Actively Involved
- Customers and Personnel Information
- Electronic, Paper and Other Media
- Don’t shelf policies and procedures–update them!
- Awareness training and updates for all employees—even executives
- Have a Retention Program (electronic, paper and other media)

Your Privacy Plan

- Foster a Privacy Culture
  - Recognize who handles the information
    - Entry level personnel
    - Important to engage in the program
    - Temps (special issues can arise)
  - Role based access and minimum necessary principles
  - Disclosure of information—is all personal information needed or only portions?
  - Have redaction training and procedures

Your Privacy Plan

- Culture of Privacy--Employees
  - Continued Awareness
    - Training on Hire and Annually
    - Special training for certain areas
    - Confidentiality and Non-disclosure statements
    - Employee evaluations
    - Supervisors accountable
    - Awards and contests for ideas

Your Privacy Plan

- Personnel Records
  - What are supervisors keeping at desks—personal/medical information??
  - Special training for HR folks
  - HIPAA coverage
    - Generally not applied to employers
    - Will apply to records needed for work determinations
    - Will apply to sponsored and self-insured benefit plans
    - Don’t use for employment decisions!!!

Your Privacy Plan

- Contracts
  - Vendors use (research??)
  - Purchase Orders—be cautious!
  - Scope of Work (be specific with data, access and responsibilities)
  - Non-disclosure Agreements
  - Data breach notification to company and to customers as determined by company and contractor
  - Company retains right to any part of investigation by contractor

Your Privacy Plan

- Digitizing records and plan for use
  - Are these records being uploaded to web sites???
  - Have they been classified for purposes of the Arizona Public Records Act??
  - Retention plan
  - E-discovery

Your Privacy Plan

- Investigation
  - What information is missing (reconstruct)
  - How long?
  - Where from?
  - Who had access?
  - Must be prompt investigation
  - Notify risk management, legal counsel, executive management and if a state agency, SISPO
  - Lessons learned and remediation

Your Privacy Plan

- Develop a report of concern process
  - Non-punitive
  - Anonymous reporting system
  - Policies and practices are the same—no retaliation
  - Take reports seriously
  - Termination interviews

Your Privacy Plan

- What's left out…..??

Your Privacy Plan

- What's left out…..?
  - Who has access to email and the network?
  - Adjunct committees and privacy

Remember

Privacy is the GOAL

Security is the journey

Technology can help

People are the key

Contact

Mary Beth Joublanc, JD

Chief Privacy Officer

State of Arizona

Statewide Information Security & Privacy Office

http://azgita.gov/sispo/

Government Information Technology Agency

100 N. 15th Ave. Suite 440

Phoenix, Arizona 85007

602.364-4537

mbjoublanc@azgita.gov